Proskauer

Wisconsin Latest State to Provide Social Media Protections to Applicants and Employees

April 14, 2014

On April 8, 2014, Governor Scott Walker signed Wisconsin Act 208 to prohibit employers from requiring or requesting that prospective and current employees disclose usernames and passwords for their personal Internet accounts. Wisconsin becomes the thirteenth state to grant similar social media protections, following New Jersey, Maryland, Illinois, California, Michigan, Utah, New Mexico, Arkansas, Colorado, Washington, Oregon and Nevada. What is more, a number of other states and the U.S. Congress are considering comparable legislation. This alert discusses the coverage, prohibitions, exceptions, and remedies of Wisconsin's new law, which took effect on April 10, 2014.[1]

Coverage

Wisconsin's new law defines "employer" as any person engaging in any activity, enterprise or business that employs at least one individual. The term specifically encompasses the state of Wisconsin, as well as any office, department or other body of the state or local government, including the legislature and courts.

Prohibitions

Pursuant to the new law, an employer may not request or require a current or prospective employee to disclose "access information"[2] for his or her "personal Internet account"[3] or to otherwise permit the employer to access or observe the account as a condition of employment. An employer also may not fail to hire an applicant for refusing to allow such access.

Employees likewise are protected from discharge or discrimination for refusing access to their personal Internet accounts, and an employer also may not retaliate against an employee for: (i) filing a complaint or attempting to enforce a right under the new law; (ii) testifying or assisting in any action or proceeding to enforce a right under the new law; or (iii) otherwise opposing a practice prohibited under the new law.

By amending Wisconsin's existing employment discrimination statute, the new law also prohibits employers from bargaining with a collective bargaining unit so as to provide employees with fewer rights and protections than to which they would otherwise be entitled under the new law.

Exceptions

Wisconsin's new law specifically permits employers to:

- Request or require an employee to disclose access information for (i) an electronic communications device supplied or paid for, in whole or in part, by the employer, or (ii) accounts or services provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes;
- Discharge or discipline an employee for transferring the employer's proprietary, confidential, or financial information to his or her personal Internet account without authorization;
- Conduct an investigation or require an employee to cooperate in an investigation where there is reasonable cause to believe that the employee (i) transferred the employer's proprietary, confidential or financial information to a personal Internet account, (ii) engaged in other employment-related misconduct, or (iii) violated the law or workplace rules as specified in an employee handbook. As part of the investigation, an employer may require an employee to grant access to, or allow observation of, his or her personal Internet account, but may not require the employee to disclose access information for that account;
- Restrict or prohibit access to certain Internet sites while using the employer's network or an electronic communications device supplied or paid for, in whole or in part, by the employer;
- Screen applicants prior to hiring, or monitor or retain employee communications, pursuant to a duty imposed under state or federal laws, rules or regulations, or the rules of a self-regulatory organization (as defined by federal law);
- View, access, or use information about current or prospective employees that the employer can obtain without access information or through the public domain; or
- Request or require an employee to disclose a personal email address.

The new law specifies that it does not apply to a personal Internet account or an electronic communications device of an employee in the financial services industry who uses the account or device to conduct the business of an employer subject to federal securities laws and regulations or the rules of a self-regulatory organization (as defined by federal law).

Moreover, the new law makes clear that an employer does not violate its provisions by inadvertently obtaining access information for an employee's personal Internet account through the use of an electronic device that monitors the employer's network or through an electronics communication device supplied or paid for, in whole or in part, by the employer, so long as the employer does not use that information to access the employee's account.

Remedies

An employer who violates the new law may be required to "forfeit" no more than $1,000. In addition, an aggrieved employee or applicant may file a complaint with the Wisconsin Department of Workforce Development Division of Equal Rights ("Division") when the employer has refused to hire, retaliated or otherwise discriminated against the individual for exercising his or her rights under the statute. The complaint procedure is the same as under Wisconsin's existing discrimination law, which provides prevailing complainants with remedies that may include reinstatement or compensatory damages of no less than 500 times but no more than 1,000 times the employee's hourly wage at the time the violation occurred.[4]

Takeaway

To ensure compliance with the new law, Wisconsin employers should review their hiring, monitoring, and investigatory procedures regarding the use of social media, and make any necessary changes. Regardless of the scope of remedies under the new law, employers should be aware that engaging in the type of conduct the new law prohibits may give rise to substantial damages under other laws. Indeed, recent federal case law suggests that employers who access employees' personal social media accounts without authorization may run afoul of federal statutes such as the Stored Communications Act, as well as common law privacy rights. Furthermore, although the new law permits employers to view publically accessible profiles, employers should recognize that such conduct may give rise to a discrimination claim under Title VII of the Civil Rights Act of 1964 or a state equivalent if the employer takes adverse action based on information that reveals a protected characteristic such as race or religion.

Given these risks, Wisconsin employers should adopt a clear and compliant workplace policy governing the use of social media. Please contact your Proskauer relationship lawyer if you have any questions about the new law or social media policies.

[1] Where an existing CBA is inconsistent with Wisconsin's new law, the law will apply to employees on the first day on which the CBA expires, or is extended, modified or renewed, whichever occurs first.

[2] The new law defines "access information" as a user name and password or any other security information that protects access to a "personal Internet account."

[3] The new law defines "personal Internet account" as any Internet-based account created and used by an individual exclusively for purposes of personal communications.

[4] Although arguably unclear, the $1,000 maximum "forfeiture" appears to be a standalone penalty that does not impose a cap on damages that would otherwise be available to an aggrieved individual when filing a complaint with the Division.

***Authors of this alert**:*

Katharine H. Parker, Daniel L. Saperstein, Kelly Anne Targett and Allison Lynn Martin.